# STATISTICS OF THE JACOBIANS OF HYPERELLIPTIC CURVES OVER FINITE FIELDS

MAOSHENG XIONG AND ALEXANDRU ZAHARESCU*

Abstract. Let $C$ be a smooth projective curve of genus $g \geq 1$ over a finite field $\mathbb{F}_q$ of cardinality $q$. In this paper, we first study $\#\mathcal{J}_C$, the size of the Jacobian of $C$ over $\mathbb{F}_q$ in case that $\mathbb{F}_q(C)/\mathbb{F}_q(X)$ is a geometric Galois extension. This improves results of Shparlinski [19]. Then we study fluctuations of the quantity $\log \#\mathcal{J}_C - g \log q$ as the curve $C$ varies over a large family of hyperelliptic curves of genus $g$. For fixed genus and growing $q$, Katz and Sarnak showed that $\sqrt{q}\,(\log \#\mathcal{J}_C - g \log q)$ is distributed as the trace of a random $2g \times 2g$ unitary symplectic matrix. When the finite field is fixed and the genus grows, we find the limiting distribution of $\log \#\mathcal{J}_C - g \log q$ in terms of the characteristic function. When both the genus and the finite field grow, we find that $\sqrt{q}\,(\log \#\mathcal{J}_C - g \log q)$ has a standard Gaussian distribution.

## 1. Introduction

Let $C$ be a smooth projective curve of genus $g \geq 1$ over a finite field $\mathbb{F}_q$ of cardinality $q$. The Jacobian $\mathrm{Jac}(C)$ is a $g$-dimensional abelian variety. The set of the $\mathbb{F}_q$-rational points on $\mathrm{Jac}(C)$, denoted by $\mathcal{J}_C = \mathrm{Jac}(C)(\mathbb{F}_q)$, is a finite abelian group. The group $\mathcal{J}_C$ has been studied extensively, partly because of its importance in the theory of algebraic curves and its surprising applications in public-key cryptography and computational number theory. For example, such groups are extremely useful in primality testing [3] and integer factorization [11, 12]. Statistics of group structures of $\mathcal{J}_C$, for instance the analogue of the Cohen-Lenstra conjecture over function fields

2000 *Mathematics Subject Classification.* 11G20,11T55,11M38.
*Key words and phrases.* zeta functions of curves, class number, Jacobian, Gaussian distribution.
*The second author was supported by NSF grant number DMS-0901621.

remains an inspiring problem in number theory and provides insight for number fields case. Interested readers may refer to [1, 2, 22] for details and current development. The main purpose of this paper is to study $\#J_C$, the size of the Jacobian over $\mathbb{F}_q$. This quantity is also the class number of the function field $\mathbb{F}_q(C)$ ([17, Theorem 5.9]), a subject of study with a rich history.

The zeta function of $C/\mathbb{F}_q$ is a rational function of the form

$$Z_C(u) = \frac{P_C(u)}{(1-u)(1-qu)},$$

where $P_C(u) \in \mathbb{Z}[u]$ is a polynomial of degree $2g$ with $P_C(0) = 1$, satisfying the functional equation

$$P_C(u) = \left(qu^2\right)^g P_C\left(\frac{1}{qu}\right),$$

and having all its zeros on the circle $|u| = 1/\sqrt{q}$ (the Riemann Hypothesis for curves [23]). Moreover, there is a unitary symplectic matrix $\Theta_C \in \mathrm{USp}(2g)$, defined up to conjugacy, so that

$$P_C(u) = \det\left(I - u\sqrt{q}\Theta_C\right).$$

The eigenvalues of $\Theta_C$ are of the form $e\left(\theta_{C,j}\right), j = 1, \ldots, 2g$, where $e(\theta) = e^{2\pi i\theta}$.

It is known that $\#\mathcal{J}_C = P_C(1)$ (see [13, Corollary VIII.6.3]). From this we immediately derive that

$$(q^{1/2} - 1)^{2g} \leq \#\mathcal{J}_C \leq (q^{1/2} + 1)^{2g},$$

which is tight in the case $g = 1$ due to the classical result of Deuring [6]. Many improvements of this bound have been obtained in [15, 16, 19, 20, 21]. In particular in an interesting paper [19], Shparlinski proves that if $C$ is a smooth absolutely irreducible curve of genus $g$ over $\mathbb{F}_q$ with gonality $d$, then

$$\log \#\mathcal{J}_C = g \log q + O\left(g \log^{-1}(g/d)\right) \tag{1}$$

as $g \to \infty$, where the implied constant may depend on $q$. (The gonality of a curve $C$ is the smallest integer $d$ such that $C$ admits a non-constant map of degree $d$ to the projective line over the ground field $\mathbb{F}_q$. For example, a hyperelliptic curve is a curve given by an affine model $Y^2 = F(X)$ for some $F \in \mathbb{F}_q[X]$, so the gonality is $d = 2$.) This generalizes and improves similar results of Tsfasman [21].

In this paper, we first prove that in case the function field $\mathbb{F}_q(C)$ is a geometric Galois extension of $\mathbb{F}_q(X)$, a sharper estimate can be obtained. Here "geometric" means that the constant field of $\mathbb{F}_q(C)$ is still $\mathbb{F}_q$.

**Theorem 1.** *Let $C$ be a smooth projective curve of genus $g \geq 1$ over $\mathbb{F}_q$. Assume that the function field $\mathbb{F}_q(C)$ is a geometric Galois extension of the rational function field $\mathbb{F}_q(X)$ with $N = \#\mathrm{Gal}\,(\mathbb{F}_q(C)/F[X])$. Then*

$$|\log \#\mathcal{J}_C - g \log q| \leq (N-1)\left(\log \max\left\{1, \frac{\log(7g/(N-1))}{\log q}\right\} + 3\right). \tag{2}$$

We remark that in Theorem 1, the inequality (2) is explicit and holds true for any $g$ and $q$. Moreover, the quantity $\log \#\mathcal{J}_C - g \log q$ is essentially bounded by $O(\log \log g)$, which is significantly smaller than $O(g/\log g)$ implied from (1).

Now assume that $q$ is odd. For each positive integer $d \geq 3$, denote by $\mathcal{H}_{d,q}$ the family of hyperelliptic curves having an affine equation of the form $Y^2 = F(X)$, with $F \in \mathbb{F}_q[X]$ a monic square-free polynomials of degree $d$. The measure on $\mathcal{H}_{d,q}$ is simply the uniform probability measure on the set of such polynomials. The genus of a curve $C \in \mathcal{H}_{d,q}$ is given by

$$g = g(C) = \left[\frac{d-1}{2}\right],$$

where for $x \in \mathbb{R}$, $[x]$ denotes the largest integer not exceeding $x$. For any $C \in \mathcal{H}_{d,q}$, since $\mathbb{F}_q(C)/\mathbb{F}_q(X)$ is a geometric Galois extension with Galois group $\mathbb{Z}/2\mathbb{Z}$, Theorem

1 implies that

$$|\log \#\mathcal{J}_C - g\log q| \le \log\max\left\{1, \log\frac{\log(7g)}{\log q}\right\} + 3\,. \tag{3}$$

The inequality (3) appears to be very sharp, however we will see that for most hyperelliptic curves $C \in \mathcal{H}_{d,q}$, the value $|\log \#\mathcal{J}_C - g\log q|$ is actually much smaller. More precisely we prove the following.

**Theorem 2.** *For any $\psi \ge 2$, denote*

$$M_\psi := \#\left\{C \in \mathcal{H}_{d,q} : |\log \#\mathcal{J}_C - g\log q| \ge \psi\right\}.$$

*Then*

$$\frac{\#M_\psi}{\#\mathcal{H}_{d,q}} \ll \exp\left(-\frac{\psi}{2}\log(q\log\psi)\right),$$

*where the implied constant in "$\ll$" is absolute.*

Theorem 2 shows that the ratio $\frac{\#M_\psi}{\#\mathcal{H}_d}$ goes to zero very fast whenever $\psi$ or $q$ goes to infinity. When $q \to \infty$, this is not surprising. Actually, in this case, much more is known. Writing

$$P_C(u) = \prod_{i=1}^{2g}\left(1 - \sqrt{q}e\left(\theta_{C,i}\right)u\right),$$

then

$$\log \#\mathcal{J}_C - g\log q = \sum_{i=1}^{2g}\log\left(1 - q^{-1/2}e(\theta_{C,i})\right).$$

Katz and Sarnak [9] showed that for fixed genus $g$, the conjugacy classes $\{\Theta_C : C \in \mathcal{H}_{d,q}\}$ become uniformly distributed in $\mathrm{USp}(2g)$ in the limit $q \to \infty$. In particular, since

$$\lim_{q\to\infty}\sqrt{q}\left(\log \#\mathcal{J}_C - g\log q\right) = -\sum_{i=1}^{2g} e(\theta_{C,i}),$$

it implies that

(i). When $g$ is fixed and $q \to \infty$, the value $-\sqrt{q}\,(\log \#\mathcal{J}_C - g\log q)$ for $C \in \mathcal{H}_{d,q}$ is distributed asymptotically as the trace of a random matrix in $\mathrm{USp}(2g)$.

Furthermore, since the limiting distribution of traces of a random matrix in $\mathrm{USp}(2g)$, as $g \to \infty$, is a standard Gaussian by a theorem of Diaconis and Shahshahani [7], it also implies that

(ii). If $q \to \infty$ and then $g \to \infty$, the value $\sqrt{q}\,(\log \#\mathcal{J}_C - g\log q)$ is distributed as a standard Gaussian.

Katz and Sarnak's powerful theorem [9] provides an almost complete story, except that in their argument, it is crucial to take the limit that $q \to \infty$. What happens if $g \to \infty$ instead? Complementary to (i) and (ii) above, we prove the following.

**Theorem 3.** *(1). If $q$ is fixed and $g \to \infty$, then for $C \in \mathcal{H}_{d,q}$, the quantity $\log \#\mathcal{J}_C - g\log q + \delta_{d/2}\log(1-q^{-1})$ converges weakly to a random variable $X$, whose characteristic function $\phi(t) = \mathbb{E}\left(e^{itX}\right)$ is given by*

$$\phi(t) = 1 + \sum_{r=1}^{\infty} \frac{1}{r!} \sum_{\substack{P_1,\dots,P_r \\ distinct}} \prod_{j=1}^{r} \frac{(1-|P_j|^{-1})^{-it} + (1+|P_j|^{-1})^{-it} - 2}{2\,(1+|P_j|^{-1})}, \quad \forall t \in \mathbb{R},$$

*where*

$$\delta_\gamma = \begin{cases} 1 & \gamma \in \mathbb{Z}, \\ 0 & \gamma \notin \mathbb{Z}, \end{cases}$$

*and the sum on the right over $P_1, \dots, P_r$ is over all distinct monic irreducible polynomials $P_1, \dots, P_r \in \mathbb{F}_q[X]$ and $|P_j| = q^{\deg P_j}$.*

*(2). If both $q, g \to \infty$, then for $C \in \mathcal{H}_{d,q}$, $\sqrt{q}\,(\log \#\mathcal{J}_C - g\log q)$ is distributed as a standard Gaussian, that is, for any $\gamma \in \mathbb{R}$, we have*

$$\lim_{\substack{q\to\infty \\ g\to\infty}} \frac{1}{\#\mathcal{H}_{d,q}} \#\left\{C \in \mathcal{H}_{d,q} : \sqrt{q}\,(\log \#\mathcal{J}_C - g\log q) \le \gamma\right\} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\gamma} e^{-\frac{t^2}{2}}\,\mathrm{d}t\,.$$

We remark that first, Theorem 3 is in the spirit of Kurlberg and Rudnick [10] and Faifman and Rudnick [8], who initiated the investigation of such problems. It

is also in the spirit of Bucur, David, Feigon and Lalín [4, 5], who made further important development. The proof of Theorem 3 depends heavily on techniques developed by Rudnick [18] and Faifman and Rudnick [8]. Second, (2) of Theorem 3 is slightly more general than Statement (ii) above as there is no requirement that $q \to \infty$ first. Finally, instead of averaging over $\mathcal{H}_{d,q}$, the family of hyperelliptic curves arising from monic square-free polynomials of degree $d$, the proof of Theorem 3 can be easily adapted to the moduli space of hyperelliptic curves of a fixed genus. Interested readers may refer to [4, 5] for terminology and treatment.

We organize this paper as follows. In Section 2 we collect several results which will be used later. Then we prove Theorem 1 in Section 3, Theorem 2 in Section 4 and Theorem 3 in Section 5 respectively. The proofs of Theorem 2 and Theorem 3 rely on Proposition 1–3 which are of technical natural. To emphasis and streamline the main ideas, we deal with these three propositions in Section 6.

## 2. Preliminaries

In this section we collect several results which will be used later. Interested readers can refer to [17] for more details.

2.1. **Zeta functions of function fields.** Let $K = \mathbb{F}_q(X)$ be the rational function field over the finite field $\mathbb{F}_q$ and let $L/K$ be a finite geometric Galois extension. Here "geometric" means that the constant field of $L$ is still $\mathbb{F}_q$. We list several facts about such extensions $L/K$ as follows (see [17, Chapter 9] for more details).

First, the zeta function $\zeta_L(s)$ of $L$ is defined by

$$\zeta_L(s) = \prod_{P \in \mathcal{S}_L} \left(1 - |P|^{-s}\right)^{-1},$$

where the product is over $\mathcal{S}_L$, the set of all primes of $L$, and for each $P \in \mathcal{S}_L$, $|P|$ is the cardinality of the residue field of $L$ at $P$. For the rational function field $K$, the

zeta function $\zeta_K(s)$ turns out to be

$$\zeta_K(s) = \left(1 - q^{-s}\right)^{-1} \left(1 - q^{1-s}\right)^{-1} .$$

If $C$ is a smooth projective curve of genus $g \geq 1$ over $\mathbb{F}_q$ with function field $\mathbb{F}_q(C) = L$, then $Z_C\left(q^{-s}\right) = \zeta_L(s)$, i.e., the zeta function of the curve $C$ coincides with the zeta function of the function field $\mathbb{F}_q(C)$ (see [17, pp. 57, Chap 5] for details).

Let $G = \mathrm{Gal}(L/K)$ be the Galois group of $L/K$ and $\rho : G \to \mathrm{Aut}_{\mathbb{C}}(V)$ a representation of $G$, where $V$ is a finite-dimensional vector space over the complex numbers $\mathbb{C}$ of dimension $m$. One defines the Artin L-series associated to the representation $\rho$ as follows.

If $P$ is a prime of $K$ which is unramified in $L$ and $\mathcal{B}$ is a prime of $L$ lying above $P$, one defines the local factor $L_P(s, \rho)$ as

$$L_P(s, \rho) = \det\left(I - \rho((\mathcal{B}, L/K))|P|^{-s}\right)^{-1} , \tag{4}$$

where $I$ is the identity automorphism on $V$ and $(\mathcal{B}, L/K) \in G$ is the Frobenius automorphism at $\mathcal{B}$. Since $L/K$ is Galois, this definition does not depend on the choice of $\mathcal{B}$ over $P$.

Let $\{\alpha_1(P), \alpha_2(P), \ldots, \alpha_m(P)\}$ be the eigenvalues of $\rho((\mathcal{B}, L/K))$. In terms of these eigenvalues, we get another useful expression for $L_P(s, \rho)$:

$$L_P(s, \rho)^{-1} = \left(1 - \alpha_1(P)|P|^{-s}\right)\left(1 - \alpha_2(P)|P|^{-s}\right) \cdots \left(1 - \alpha_m(P)|P|^{-s}\right) .$$

We note that these eigenvalues $\alpha_i(P)$ are all roots of unity because $(\mathcal{B}, L/K)$ has finite order.

At a prime $P$ of $K$ which is ramified in $L$, the local factor $L_P(s, \rho)$ can also be defined. The definition is similar to (4), except that the action $\rho((\mathcal{B}, L/K))$ is restricted to a subspace of $V$ which is fixed by the inertial group $I(\mathcal{B}/P)$. We are contended with the fact that there are only finitely many primes $P$ which are

ramified in $L$ and in either case we can write $L_P(s,\rho)$ as

$$L_P(s,\rho)^{-1} = \left(1-\alpha_1(P)|P|^{-s}\right)\left(1-\alpha_2(P)|P|^{-s}\right)\cdots\left(1-\alpha_m(P)|P|^{-s}\right),$$

where the values $\alpha_i(P)$'s are either roots of unity or zero. The Artin L-series $L(s,\rho)$ is defined by the infinite product

$$L(s,\rho) = \prod_{P\in\mathcal{S}_K} L_P(s,\rho),$$

where $\mathcal{S}_K$ is the set of all primes in $K=\mathbb{F}_q(X)$.

It is known that if $\rho=\rho_0$, the trivial representation, then $L(s,\rho_0)=\zeta_K(s)$, and if $\rho=\rho_{\rm reg}$, the regular representation, then $L(s,\rho_{\rm reg})=\zeta_L(s)$. It is also known that $L(s,\rho)$ depends only on the character $\chi$ of $\rho$, so we can write it as $L(s,\chi)$.

Finally, let $L/K$ be a finite, geometric and Galois extension with Galois group $G=\mathrm{Gal}(L/K)$. Let $\{\chi_1,\chi_2,\dots,\chi_h\}$ be the set of irreducible characters of $G$. We set $\chi_1=\chi_0$, the trivial character. Denote by $d_i$ the degree of $\chi_i$, i.e., $d_i=\chi_i(e)$ is the dimension of the representation space corresponding to $\chi_i$. Then using results about group characters and formal properties of Artin L-series, one derives that

$$\zeta_L(s) = \zeta_K(s)\prod_{i=2}^{h} L(s,\chi_i)^{d_i}\,. \tag{5}$$

2.2. **Averaging over $\mathcal{H}_{d,q}$.** Let $\mathcal{H}_{d,q}\subset\mathbb{F}_q[X]$ be the set of all monic square-free polynomials of degree $d\geq 3$.

**Lemma 1.** *For any Dirichlet character $\chi:\mathbb{F}_q[X]\to\mathbb{C}$ modulo $f\in\mathbb{F}_q[X]$, we have*

$$\frac{1}{\#\mathcal{H}_{d,q}}\sum_{F\in\mathcal{H}_{d,q}}\chi(F) \leq \frac{2^{\deg f-1}}{(1-q^{-1})\,q^{d/2}}\,.$$

**Proof.** This is [8, Lemma 3.1], which proves the case when $\chi = \left(\frac{f}{\cdot}\right)$ is a quadratic character. For the general case, the proof follows exactly the same line of argument, so we omit the details here. □

**Lemma 2.** *Let $h \in \mathbb{F}_q[X]$ be a monic square-free polynomial. Then*

$$\frac{1}{\#\mathcal{H}_{d,q}} \sum_{\substack{F \in \mathcal{H}_{d,q} \\ \gcd(F,h)=1}} 1 = \prod_{P|h} \left(1 + |P|^{-1}\right)^{-1} + O\left(q^{-d/2}\sigma(h)\right) ,$$

*where $\sigma(h) = \sum_{D|h} 1$.*

**Proof.** This is essentially [18, Lemma 5], which treats the case that $h = P$ is a monic irreducible polynomial. In fact in this case [18, Lemma 5] yields a much stronger error term $O(q^{-d})$. The extra saving is obtained by carefully analyzing the functional equation of the zeta function. To get the error term $O(q^{-d/2}\sigma(h))$, the proof follows a standard procedure which is included [18, Lemma 5]. We also omit details here. □

## 3. Proof of Theorem 1

Let $C$ be a smooth projective curve of genus $g \geq 1$ over $\mathbb{F}_q$. The zeta function $Z_C(u)$ is of the form

$$Z_C(u) = \frac{P_C(u)}{(1-u)(1-qu)} ,$$

where $P_C(u) \in \mathbb{Z}[u]$ is a polynomial of degree $2g$ with $P_C(0) = 1$, satisfying the functional equation

$$P_C(u) = \left(qu^2\right)^g P_C\left(\frac{1}{qu}\right) ,$$

and having all its zeros on the circle $|u| = 1/\sqrt{q}$. We may write $P_C(u)$ as

$$P_C(u) = \prod_{i=1}^{2g} \left(1 - \sqrt{q}e(\theta_i)u\right) ,$$

where these $\theta_i \in [0, 1)$ and $e(\alpha)$ stands for $e^{2\pi i\alpha}$ for any $\alpha \in \mathbb{R}$.

Since $\#\mathcal{J}_C = P_C(1)$, we have

$$\#\mathcal{J}_C = \prod_{i=1}^{2g} (1 - \sqrt{q}e(\theta_i)) = q^g \prod_{i=1}^{2g} \left(1 - q^{-1/2}e(\theta_i)\right) .$$

Taking logarithms on both sides and using the expansion

$$-\log(1-z) = \sum_{n\geq 1} \frac{z^n}{n}, \quad |z| < 1, \tag{6}$$

we obtain the equation

$$\log \#\mathcal{J}_C - g\log q = \sum_{n\geq 1} q^{-n/2} n^{-1} \sum_{i=1}^{2g} -e(n\theta_i) . \tag{7}$$

Denote $L = \mathbb{F}_q(C)$ and $K = \mathbb{F}_q(X)$. The zeta functions of $L$ and $K$ can be written as

$$\zeta_L(s) = (1-q^{-s})^{-1}(1-q^{1-s})^{-1} \prod_{i=1}^{2g} \left(1 - \sqrt{q}e(\theta_i)q^{-s}\right),$$

and

$$\zeta_K(s) = (1-q^{-s})^{-1}(1-q^{1-s})^{-1} .$$

Since $L/K$ is a geometric Galois extension with $G = \mathrm{Gal}(L/K)$ and $\#G = N$, let $\{\chi_1, \chi_2, \ldots, \chi_h\}$ be the set of irreducible characters of $G$ with $\chi_1 = \chi_0$, the trivial character and denote by $d_i$ the degree of $\chi_i$. From (5) we find that

$$\prod_{i=2}^{h} L(s,\chi_i)^{d_i} = \prod_{i=1}^{2g} \left(1 - \sqrt{q}e(\theta_i)q^{-s}\right), \tag{8}$$

where for each $i$ with $2 \leq i \leq h$, the Artin L-series associated to $\chi_i$ can be written as

$$L(s,\chi_i)^{-1} = \prod_P \left(1 - \alpha_{i,1}(P)|P|^{-s}\right)\left(1 - \alpha_{i,2}(P)|P|^{-s}\right)\cdots\left(1 - \alpha_{i,d_i}(P)|P|^{-s}\right) .$$

Here the product is over all monic irreducible polynomials $P \in \mathbb{F}_q(X)$ and $P = \infty$ with $|P| = q^{\deg P}$ ($\deg \infty = 1$ hence $|\infty| = q$) and these $\alpha_{i,j}(P)$'s are either roots of unity or zero.

Taking logarithms on both sides of (8), using the expansion (6) again and equating the coefficients, we obtain for any positive integer $n$ the identity

$$q^{n/2} \sum_{j=1}^{2g} -e(n\theta_i) = \sum_{\deg f = n} \Lambda(f) \sum_{i=2}^{h} d_i \sum_{j=1}^{d_i} \alpha_{i,j}(f)\,, \tag{9}$$

where the sum on the right side over $\deg f = n$ is over all monic polynomials $f \in \mathbb{F}_q[X]$ with $\deg f = n$, $\Lambda(f) = \deg P$ if $f = P^k$ is a prime power, and $\Lambda(f) = 0$ otherwise.

Let $Z$ be a positive integer which will be chosen later. Denote

$$\epsilon_{1,Z} = \sum_{n \le Z} q^{-n/2} n^{-1} \sum_{i=1}^{2g} -e(n\theta_i),$$

and

$$\epsilon_{2,Z} = \sum_{n > Z} q^{-n/2} n^{-1} \sum_{i=1}^{2g} -e(n\theta_i).$$

From (7) we can write

$$\log \#\mathcal{J}_C - g \log q = \epsilon_{1,Z} + \epsilon_{2,Z}\,.$$

If $Z \ge 2$ we have

$$|\epsilon_{2,Z}| \le \sum_{n \ge Z+1} q^{-n/2} n^{-1} 2g \le \frac{2g}{Z+1}\, q^{-(Z+1)/2} \left(1 - q^{-1/2}\right)^{-1}, \tag{10}$$

and if $Z = 1$ we have

$$|\epsilon_{2,Z}| \le 2g \left(-\log\left(1 - q^{-1/2}\right) - q^{-1/2}\right) \le \frac{2g}{q - \sqrt{q}}\,. \tag{11}$$

For $\epsilon_{1,Z}$, we use the identity (9). Since $|\alpha_{i,j}| \leq 1$ for all $i, j$, we obtain the inequality

$$|\epsilon_{1,Z}| \leq \sum_{n \leq Z} q^{-n} n^{-1} \sum_{\deg f = n} \Lambda(f) \sum_{i=2}^{h} d_i^2 \,.$$

It is known that

$$1 + \sum_{i=2}^{h} d_i^2 = N = \#G$$

and

$$\sum_{\deg f = n} \Lambda(f) = q^n + 1.$$

Here the extra "1" on the right side in the above equation accounts for $f = \infty^n$. Hence

$$|\epsilon_{1,Z}| \leq (N-1) \left( \sum_{n \leq Z} \frac{1}{n} + \sum_{n \leq Z} \frac{1}{nq^n} \right) .$$

If $Z = 1$, this is

$$|\epsilon_{1,Z}| \leq (N-1) \left(1 + q^{-1}\right), \tag{12}$$

and if $Z \geq 2$, we use

$$\sum_{n \leq Z} \frac{1}{n} \leq 1.5 + \log Z - \log 2$$

and

$$\sum_{n \leq Z} \frac{1}{nq^n} \leq -\log\left(1 - q^{-1}\right) \leq \frac{1}{q-1}$$

to obtain

$$|\epsilon_{1,Z}| \leq (N-1) \left(1.5 - \log 2 + \frac{1}{q-1} + \log Z\right), \quad Z \geq 2 \,. \tag{13}$$

Case 1: if $2\left(1 - q^{-1/2}\right)^{-1} g \geq (N-1)q$, we choose

$$Z = \left[ \frac{2 \log \frac{2\left(1-q^{-1/2}\right)^{-1} g}{N-1}}{\log q} \right] \geq 2 \,.$$

We find from (13) that

$$|\epsilon_{1,Z}| \le (N-1)\left\{1.5 + \frac{1}{q-1} + \log\left(\frac{\log \frac{2\left(1-q^{-1/2}\right)^{-1} g}{N-1}}{\log q}\right)\right\}$$

and from (10) that

$$|\epsilon_{2,Z}| \le \frac{N-1}{2}\,.$$

In this case noticing that $q \ge 2$, we obtain

$$|\log \#\mathcal{J}_C - g\log q| \le (N-1)\left(\log\left(\frac{\log \frac{7g}{N-1}}{\log q}\right) + 3\right)\,.$$

Case 2: if $2\left(1-q^{-1/2}\right)^{-1} g < (N-1)q$, we choose $Z = 1$, and from (12) and (11) we obtain that

$$|\log \#\mathcal{J}_C - g\log q| \le (N-1)\left(2+q^{-1}\right) < 3(N-1)\,.$$

In either case we conclude that

$$|\log \#\mathcal{J}_C - g\log q| \le (N-1)\left(\log \max\left\{1, \frac{\log(7g/(N-1))}{\log q}\right\} + 3\right)\,.$$

This completes the proof of Theorem 1. □

## 4. Proof of Theorem 2

4.1. **Preparation.** Let $\mathbb{F}_q$ be a finite field of cardinality $q$ with $q$ odd. Denote

$$\mathcal{H}_{d,q} = \{F \in \mathbb{F}_q[X] : F \text{ is monic, square-free and} \deg F = d\}\,.$$

For any $F \in \mathcal{H}_{d,q}$, the hyperelliptic curve $C_F$ is given by the affine model

$$C_F : Y^2 = F(X).$$

It has genus

$$g = g_{_F} = \left[\frac{d-1}{2}\right].$$

Suppose that the zeta function $Z_{C_F}(u)$ is of the form

$$Z_{C_F}(u) = \frac{\prod_{i=1}^{2g}\left(1-\sqrt{q}e\left(\theta_{i,F}\right)u\right)}{(1-u)(1-qu)},$$

where the $\theta_{i,F}$'s are real numbers. Then

$$\#\mathcal{J}_{C_F} = \prod_{i=1}^{2g}\left(1-\sqrt{q}e\left(\theta_{i,F}\right)\right) = q^g\prod_{i=1}^{2g}\left(1-q^{-1/2}e\left(\theta_{i,F}\right)\right).$$

Taking logarithms on both sides we obtain the equation

$$\log\#\mathcal{J}_{C_F} - g\log q = \sum_{n\geq 1} q^{-n/2}n^{-1}\sum_{i=1}^{2g} -e\left(n\theta_{i,F}\right).$$

Let $Z$ be a positive integer which will be chosen later. We write

$$\log\#\mathcal{J}_{C_F} - g\log q = \sum_{n\leq Z} q^{-n/2}n^{-1}\sum_{i=1}^{2g} -e\left(n\theta_{i,F}\right) + \epsilon_{1,Z}(F), \tag{14}$$

where

$$\epsilon_{1,Z}(F) = \sum_{n>Z} q^{-n/2}n^{-1}\sum_{i=1}^{2g} -e\left(n\theta_{i,F}\right).$$

It is easy to see that

$$|\epsilon_{1,Z}(F)| \leq \sum_{n>Z} q^{-n/2}n^{-1}2g \leq \frac{9g}{Z}\, q^{-Z/2}.$$

Denote $L = \mathbb{F}_q(C_F)$ and $K = \mathbb{F}_q(X)$. Since $L/K$ is a geometric quadratic extension and the Legendre symbol $\chi := \left(\frac{F}{\cdot}\right)$ generates the Galois group $\mathrm{Gal}(L/K)$, from (5) we have

$$L\left(s,\chi\right) = \prod_{i=1}^{2g}\left(1-\sqrt{q}e\left(\theta_{i,F}\right)q^{-s}\right), \tag{15}$$

and by definition

$$L(s,\chi) = \prod_P \left(1 - \left(\frac{F}{P}\right)|P|^{-s}\right)^{-1}. \tag{16}$$

Here the product is over all monic irreducible polynomials $P \in \mathbb{F}_q(X)$ and $P = \infty$ with $|P| = q^{\deg P}$ ($\deg \infty = 1$ hence $|\infty| = q$).

Computing $\frac{\mathrm{d}}{\mathrm{d}s}L(s,\chi)$ in two different ways using (15) and (16) and equating the coefficients we obtain for each positive integer $n$ the identity

$$\sum_{i=1}^{2g} -e\left(n\theta_{i,F}\right) = q^{-n/2} \sum_{\deg f = n} \Lambda(f)\left(\frac{F}{f}\right) + q^{-n/2}\delta_{d/2}\,, \tag{17}$$

where the sum over $\deg f = n$ on the right side is over all monic polynomials $f \in \mathbb{F}_q[X]$ with $\deg f = n$, and for any $\gamma \in \mathbb{R}$, $\delta_\gamma = 1$ if $\gamma \in \mathbb{Z}$, and $\delta_\gamma = 0$ if $\gamma \notin \mathbb{Z}$. The extra term $q^{-n/2}\delta_{n/2}$ comes from $f = \infty^n$, noting the fact that $F \in \mathcal{H}_{d,q}$ is monic and

$$\left(\frac{F}{\infty}\right) = \begin{cases} 1 & : \quad \deg F \equiv 0 \pmod 2, \\ 0 & : \quad \deg F \equiv 1 \pmod 2. \end{cases}$$

Using the identity (17) in (14) and denoting

$$N_F = \log \#\mathcal{J}_{C_F} - g\log q + \delta_{d/2}\log\left(1 - q^{-1}\right),$$

we find that

$$N_F = \triangle_Z(F) + \epsilon_Z(F),$$

where

$$\triangle_Z(F) = \sum_{n \le Z} q^{-n} n^{-1} \sum_{\deg f = n} \Lambda(f)\left(\frac{F}{f}\right), \tag{18}$$

and

$$|\epsilon_Z(F)| \le \frac{10g}{Z}\, q^{-Z/2}\,. \tag{19}$$

An upper bound for $\triangle_Z(F)$ is given by

$$|\triangle_Z(F)| \le \sum_{n\le Z} q^{-n} n^{-1} \sum_{\deg f = n} \Lambda(f) \le 1 + \log Z\,,$$

and this can be used to estimate the quantity $N_F$ (as in the proof of Theorem 1). Extra savings can be obtained by taking high moments of $N_F$ and then averaging over the set $\mathcal{H}_{d,q}$.

4.2. **The $r$-th moment $\triangle_Z$.** For any function $\chi : \mathcal{H}_d \to \mathbb{C}$, we denote by $\langle\chi\rangle$ the mean value of $\chi$ on $\mathcal{H}_{d,q}$, that is,

$$\langle\chi\rangle := \frac{1}{\#\mathcal{H}_{d,q}} \sum_{F\in\mathcal{H}_{d,q}} \chi(F)\,.$$

Assume that $d \ge 100$. We choose $r$ to be any positive even integer in the range

$$4 \le r \le \log d\,. \tag{20}$$

We will estimate the $r$-moment $\langle(\triangle_Z)^r\rangle$ first.

From (18),

$$\triangle_Z(F)^r = \sum_{n_1,\dots,n_r\le Z} \prod_{i=1}^{r} q^{-n_i} n_i^{-1} \sum_{\substack{\deg f_i = n_i\\ 1\le i\le r}} \Lambda(f_1)\cdots\Lambda(f_r) \left(\frac{F}{f_1\cdots f_r}\right)\,,$$

hence

$$\langle(\triangle_Z)^r\rangle = \sum_{n_1,\dots,n_r\le Z} \prod_{i=1}^{r} q^{-n_i} n_i^{-1} \sum_{\substack{\deg f_i = n_i\\ 1\le i\le r}} \Lambda(f_1)\cdots\Lambda(f_r) \left\langle\left(\frac{\cdot}{f_1\cdots f_r}\right)\right\rangle\,.$$

If $f_1 \cdots f_r$ is not a square in $\mathbb{F}_q[X]$, then $\left(\frac{\cdot}{f_1 \cdots f_r}\right) : \mathbb{F}_q[X] \to \mathbb{C}$ is a non-trivial Dirichlet character modulo $h$ with $\deg h \leq \sum_{i=1}^{r} \deg f_i$, by Lemma 1 we find that

$$\left\langle \left(\frac{\cdot}{f_1 \cdots f_r}\right) \right\rangle \leq \frac{2^{n_1+\cdots+n_r-1}}{(1-q^{-1})\, q^{d/2}}\,.$$

The total contribution to $\langle (\triangle_Z)^r \rangle$ from this case is bounded by

$$T_1 \leq \sum_{n_1,\ldots,n_r \leq Z} \prod_{i=1}^{r} q^{-n_i} n_i^{-1} \sum_{\substack{\deg f_i = n_i \\ 1 \leq i \leq r}} \Lambda(f_1) \cdots \Lambda(f_r) \frac{2^{n_1+\cdots+n_r-1}}{(1-q^{-1})\, q^{d/2}}.$$

This can be estimated as

$$T_1 \leq \frac{q^{-d/2} 2^{(Z+1)r}}{2\,(1-q^{-1})} \leq q^{-d/2} 2^{(Z+1)r}\ . \tag{21}$$

If $f_1 \cdots f_r$ is a square in $\mathbb{F}_q[X]$, denote $f_1 \cdots f_r = h^2$ and $\widetilde{h} = \prod_{P|h} P$, then $\left(\frac{\cdot}{h^2}\right)$ is a trivial character, by Lemma 2 we find that

$$\left\langle \left(\frac{\cdot}{h^2}\right) \right\rangle = \frac{1}{\#\mathcal{H}_{d,q}} \sum_{\substack{F \in \mathcal{H}_{d,q} \\ \gcd(F,\widetilde{h})=1}} 1 = \prod_{P|\widetilde{h}} \left(1 + |P|^{-1}\right)^{-1} + O\left(q^{-d/2}\sigma(\widetilde{h})\right)\,.$$

Since $f_i$'s are always prime powers, $\sigma(\widetilde{h}) \leq 2^r$. The total contribution to $\langle (\triangle_Z)^r \rangle$ from the error term $O\left(q^{-d/2}\sigma(\widetilde{h})\right)$ is bounded by

$$T_2 \leq \sum_{n_1,\ldots,n_r \leq Z} \prod_{i=1}^{r} q^{-n_i} n_i^{-1} \sum_{\substack{\deg f_i = n_i \\ 1 \leq i \leq r}} \Lambda(f_1) \cdots \Lambda(f_r) q^{-d/2} 2^r.$$

This can be estimated as

$$T_2 \leq q^{-d/2} 2^r (1 + \log Z)^r\,. \tag{22}$$

The total contribution from the main term $\prod_{P|\widetilde{h}}(1+|P|^{-1})^{-1}$ is

$$\sum_{n_1,\dots,n_r\le Z}\prod_{i=1}^{r}q^{-n_i}n_i^{-1}\sum_{\substack{\deg f_i=n_i\\1\le i\le r\\ f_1\cdots f_r=h^2}}\Lambda(f_1)\cdots\Lambda(f_r)\prod_{P|h}\left(1+|P|^{-1}\right)^{-1}.$$

Removing the restrictions that $n_1,\dots,n_r\le Z$, all terms being non-negative, we can bound the above sums as

$$H(r)=\sum_{n_1,\dots,n_r\ge 1}\prod_{i=1}^{r}q^{-n_i}n_i^{-1}\sum_{\substack{\deg f_i=n_i\\1\le i\le r\\ f_1\cdots f_r=h^2}}\Lambda(f_1)\cdots\Lambda(f_r)\prod_{P|h}\left(1+|P|^{-1}\right)^{-1}. \tag{23}$$

Proposition 2 which we will prove in Section 6 provides us with the estimate

$$H(r)\le C\left(\frac{4r\log\log r}{\sqrt{q}\log r}\right)^r$$

for any positive integer $r\ge 4$, where $C>0$ is an absolute constant. Combining it with (21) and (22) we obtain

$$\langle(\triangle_Z)^r\rangle\le q^{-d/2}2^{(Z+1)r}+q^{-d/2}2^r(1+\log Z)^r+C\left(\frac{r}{\sqrt{q\log r}}\right)^r.$$

Choosing

$$Z=\left[\frac{d}{(\log d)^2}\right], \tag{24}$$

we find that

$$\langle(\triangle_Z)^r\rangle\le C\left(\frac{r}{\sqrt{q\log r}}\right)^r \tag{25}$$

for some absolute constant $C$, where the positive integer $r$ is in the range (20).

4.3. **Proof of Theorem 2.** Since $N_F=\triangle_Z(F)+\epsilon_Z(F)$, we have

$$\langle(N_F)^r\rangle=\langle(\triangle_Z)^r\rangle+E_{Z,r},$$

where

$$E_{Z,r} = \sum_{l=0}^{r-1} \binom{r}{l} \left\langle (\epsilon_Z)^{r-l} (\triangle_Z)^l \right\rangle .$$

Using (19), (20), (24) and (25) we find that

$$E_{Z,r} \leq r^{r+1} \left( \frac{10g}{Z} \; q^{-Z/2} \right) \left\langle (\triangle_Z)^{2r} \right\rangle^{1/2} \leq C \left( \frac{r}{\sqrt{q \log r}} \right)^r$$

for some absolute constant $C$. Therefore again we obtain

$$\langle (N_F)^r \rangle \leq C \left( \frac{r}{\sqrt{q \log r}} \right)^r ,$$

and the above inequality holds true for any positive even integer $r$ in the range $4 \leq r \leq \log d$ and $d \geq 100$.

For any $\psi$ with $4 \leq \psi \leq \log d$, denote

$$M_\psi = \# \left\{ F \in \mathcal{H}_{d,q} : |N_F| \geq \psi \right\} .$$

Then for any positive even integer $r$ in the range (20) we have

$$\frac{\# M_\psi}{\# \mathcal{H}_{d,q}} \; \psi^r \leq \langle (N_F)^r \rangle \leq C \left( \frac{r}{\sqrt{q \log r}} \right)^r .$$

Choosing $r \approx \psi$ we find that

$$\frac{\# M_\psi}{\# \mathcal{H}_{d,q}} \leq C \left( \frac{1}{\sqrt{q \log \psi}} \right)^\psi \ll \exp \left( -\frac{\psi}{2} \log (q \log \psi) \right) .$$

This completes the proof of Theorem 2. $\square$

## 5. Proof of Theorem 3

The proof of Theorem 3 is similar to that of Theorem 2, except that in the proof of Theorem 3, we need exact asymptotic formulas for each fixed $r$-th moment under the limit that $g \to \infty$ and both $g, q \to \infty$, instead of upper bounds as in the proof of Theorem 2. We summarize part of the proof of Theorem 2 as follows. From now

on the constants implied by the notation "$\ll$" and "$O$" may depend on the fixed positive integer $r$.

As $d \to \infty$ or $d, q \to \infty$, let $g = \left[\frac{d-1}{2}\right] \to \infty$. Choose

$$Z = \left[\frac{d}{(\log d)^2}\right]. \tag{26}$$

Denote

$$N_F = \log \#\mathcal{J}_{C_F} - g \log q + \delta_{d/2} \log\left(1 - q^{-1}\right). \tag{27}$$

Then

$$N_F = \triangle_Z(F) + \epsilon_Z(F),$$

where

$$\triangle_Z(F) = \sum_{n \le Z} q^{-n} n^{-1} \sum_{\deg f = n} \Lambda(f) \left(\frac{F}{f}\right),$$

and

$$|\epsilon_Z(F)| \le \frac{10g}{Z}\ q^{-Z/2}, \quad |\triangle_Z(F)| \ll \log Z\,. \tag{28}$$

For each positive integer $r$,

$$\langle (\triangle_Z)^r \rangle = \sum_{n_1,\dots,n_r \le Z} \prod_{i=1}^{r} q^{-n_i} n_i^{-1} \sum_{\substack{\deg f_i = n_i \\ 1 \le i \le r \\ f_1 \cdots f_r = h^2}} \Lambda(f_1)\cdots\Lambda(f_r) \prod_{P \mid h} \left(1 + |P|^{-1}\right)^{-1} + T_1 + T_2,$$

where

$$|T_1| + |T_2| \le q^{-d/2} 2^{(Z+1)r} + q^{-d/2} 2^r\,(1 + \log Z)^r \ll q^{-d/3}.$$

We can write the main term as

$$\sum_{h}\prod_{P|h}\left(1+|P|^{-1}\right)^{-1}|h|^{-2}\sum_{\substack{\deg f_i\le Z\\ 1\le i\le r\\ f_1\cdots f_r=h^2}}\frac{\Lambda(f_1)\cdots\Lambda(f_r)}{(\deg f_1)\cdots(\deg f_r)}\,.$$

Removing the restriction that $\deg f_1,\dots,\deg f_r\le Z$ results in an error bounded by

$$\sum_{\substack{h\\ \deg h>Z/2}}\prod_{P|h}\left(1+|P|^{-1}\right)^{-1}|h|^{-2}\sum_{\substack{f_1,\dots,f_r\\ f_1\cdots f_r=h^2}}\frac{\Lambda(f_1)\cdots\Lambda(f_r)}{(\deg f_1)\cdots(\deg f_r)}\,.$$

Noticing that $\frac{\Lambda(f_i)}{\deg f_i}\le 1$ and $f_i$'s are all prime powers, the sum over $h$ is actually over all monic polynomials $h\in F[X]$ with $\omega(h)\le r$ and $\deg h>Z/2$, where $\omega(h)$ is the function counting the number of distinct prime factors of $h$. If such an $h$ is chosen, the number of choices for each $f_i$ dividing $h$ which is a prime power is less than $2r\deg h$. Hence the error by removing the restriction that $\deg f_1,\dots,\deg f_r\le Z$ is bounded by

$$T_3\le\sum_{\deg h>Z/2}|h|^{-2}(2r\deg h)^r=\sum_{n>Z/2}q^{-n}(2rn)^r\ll q^{-Z/4}\,.$$

Combining these estimates together we obtain

$$\left\langle(\triangle_Z)^r\right\rangle=H(r)+T,$$

where $H(r)$ is the same function given in (23) as in the proof of Theorem 2 and $T\ll q^{-Z/4}$. As in the proof of Theorem 2, we write

$$\left\langle(N_F)^r\right\rangle=\left\langle(\triangle_Z)^r\right\rangle+E_{Z,r},$$

where

$$E_{Z,r}=\sum_{l=1}^{r}\binom{r}{l}\left\langle(\epsilon_Z)^l(\triangle_Z)^{r-l}\right\rangle\ll q^{-Z/4}\,.$$

Using (26) and (28) we find that

$$\langle (N_F)^r \rangle = H(r) + O\left(q^{-Z/4}\right). \tag{29}$$

If $q$ is fixed and $d \to \infty$, then for each fixed $r$,

$$\lim_{d\to\infty} \langle (N_F)^r \rangle = H(r).$$

Now suppose that $X$ is a random variable with

$$\mathbb{E}(X^r) = H(r), \quad \forall r \in \mathbb{N}. \tag{30}$$

For any $t \in \mathbb{R}$, the characteristic function $\phi(t)$ of $X$ is given by

$$\phi(t) = \mathbb{E}\left(e^{itX}\right).$$

Expanding $e^{itX}$ by using the identity

$$e^x = 1 + \sum_{n=1}^{\infty} \frac{x^n}{n!}, \tag{31}$$

using (30) and applying Proposition 1 for $H(r)$ which we will prove in Section 6, we find that

$$\phi(t) = 1 + \sum_{n=1}^{\infty} \frac{(it)^n}{n!} \sum_{r=1}^{\infty} \frac{n!}{2^r r!} \sum_{\substack{\lambda_1+\cdots+\lambda_r=n \\ \lambda_i \geq 1}} \sum_{\substack{P_1,\ldots,P_r \\ \text{distinct}}} \prod_{j=1}^{r} \frac{u_{P_j}^{\lambda_j} + (-1)^{\lambda_j} v_{P_j}^{\lambda_j}}{\lambda_j! \left(1 + |P_j|^{-1}\right)},$$

where for any $P \in \mathbb{F}_q[X]$,

$$u_P = -\log\left(1 - |P_j|^{-1}\right), \quad v_P = \log\left(1 + |P_j|^{-1}\right).$$

Changing the order of summation again we obtain

$$\phi(t) = 1 + \sum_{r=1}^{\infty} \frac{1}{2^r r!} \sum_{\substack{P_1,\ldots,P_r \\ \text{distinct}}} \prod_{j=1}^{r} \left( \sum_{\lambda_j=1}^{\infty} \frac{(it)^{\lambda_j} \left(u_{P_j}^{\lambda_j} + (-1)^{\lambda_j} v_{P_j}^{\lambda_j}\right)}{\lambda_j! \left(1 + |P_j|^{-1}\right)} \right).$$

The identity (31) implies that

$$\phi(t) = 1 + \sum_{r=1}^{\infty} \frac{1}{2^r r!} \sum_{\substack{P_1,\dots,P_r \\ \text{distinct}}} \prod_{j=1}^{r} \left( \frac{(1-|P_j|^{-1})^{-it} + (1+|P_j|^{-1})^{-it} - 2}{\lambda_j! \, (1+|P_j|^{-1})} \right).$$

This completes the proof of (1) of Theorem 3.

For (2) of Theorem 3, assume that both $d, q \to \infty$. Proposition 3 which we will prove in Section 6 shows that for each fixed positive integer $r$ we have

$$H(r) = \frac{\delta_{r/2} r!}{2^{r/2}(r/2)!} q^{-r/2} + O\left(q^{-(r+1)/2}\right).$$

Here the implied constant in the notation "$O$" depends on $r$. From (29) we find that for any fixed positive integer $r$

$$\langle (N_F)^r \rangle = \frac{\delta_{r/2} r!}{2^{r/2}(r/2)!} q^{-r/2} + O\left(q^{-(r+1)/2} + q^{-Z/4}\right).$$

We rewrite it as

$$\langle (\sqrt{q} N_F)^r \rangle = \frac{\delta_{r/2} r!}{2^{r/2}(r/2)!} + O\left(q^{-1/2} + q^{-(Z-2r)/4}\right).$$

Using the definition of $N_F$ in (27), letting $q, d \to \infty$, also noticing that

$$\lim_{q \to \infty} \sqrt{q} \log\left(1 - q^{-1}\right) = 0,$$

we find that all moments of $\sqrt{q}\,(\log \# J_{C_F} - g \log q)$ as $F$ varies in $\mathcal{H}_d$ are asymptotic to the corresponding moments of a standard Gaussian distribution, where the odd moments vanish and the even moments are

$$\frac{1}{\sqrt{2\pi}} \int_{\infty}^{\infty} x^{2r} e^{-x^2/2} \mathrm{d}\, x = \frac{(2r)!}{2^r r!}.$$

This implies that as $q, d \to \infty$ and $F$ varies in the set $\mathcal{H}_d$, the value $\sqrt{q}\,(\log \# J_{C_F} - g \log q)$, considered as a random variable on the space $\mathcal{H}_d$, converges weakly to a standard Gaussian variable. This completes the proof (2) of Theorem 3. □

## 6. Analysis of $H(s)$

6.1. **Proposition 1.** Let $\mathbb{F}_q$ be a finite field of cardinality $q$. For any positive integer $s$, denote

$$H(s) = \sum_{n_1,\dots,n_s\geq 1} \prod_{i=1}^{s} q^{-n_i} n_i^{-1} \sum_{\substack{\deg f_i = n_i \\ 1\leq i\leq s \\ f_1\cdots f_s = h^2}} \Lambda(f_1)\cdots\Lambda(f_s) \prod_{P|h} \left(1+|P|^{-1}\right)^{-1}.$$

We first derive another representation of $H(s)$ which is useful in the proofs of Theorems 2 and 3.

**Proposition 1.** *For any positive integer $s \geq 1$ we have*

$$H(s) = \sum_{r=1}^{s} \frac{s!}{2^r r!} \sum_{\substack{\lambda_1+\cdots+\lambda_r=s \\ \lambda_i\geq 1}} \sum_{\substack{P_1,\dots,P_r \\ distinct}} \prod_{i=1}^{r} \frac{u_{P_i}^{\lambda_i} + (-1)^{\lambda_i} v_{P_i}^{\lambda_i}}{\lambda_i! \left(1+|P_i|^{-1}\right)},$$

*where the sum on the right side is over all positive integers $\lambda_1,\dots,\lambda_r$ such that $\lambda_1+\cdots+\lambda_r = s$ and over all distinct monic irreducible polynomials $P_1,\dots,P_r \in \mathbb{F}_q[X]$, and*

$$u_P = -\log\left(1-|P|^{-1}\right), \quad v_P = \log\left(1+|P|^{-1}\right), \quad \forall P\in\mathbb{F}_q[X]. \tag{32}$$

**Proof.** We rewrite $H(s)$ as

$$H(s) = \sum_{h} \prod_{P|h} \left(1+|P|^{-1}\right)^{-1} |h|^{-2} \sum_{\substack{f_1,\dots,f_s \\ f_1\cdots f_s = h^2}} \frac{\Lambda(f_1)\cdots\Lambda(f_s)}{(\deg f_1)\cdots(\deg f_s)}.$$

Since $f_i$'s are prime powers, the sum over $h$ is actually over all monic polynomials $h\in\mathbb{F}_q[X]$ with $\omega(h)\leq r$, where $\omega(h)$ is the number of distinct prime factors of $h$. Hence

$$H(s) = \sum_{r=1}^{s} H(s,r), \tag{33}$$

where

$$H(s,r)=\sum_{\substack{h\\ \omega(h)=r}}\prod_{P|h}\left(1+|P|^{-1}\right)^{-1}|h|^{-2}\sum_{\substack{f_1,\dots,f_s\\ f_1\cdots f_s=h^2}}\frac{\Lambda(f_1)\cdots\Lambda(f_s)}{(\deg f_1)\cdots(\deg f_s)}\,.$$

If $\omega(h)=r$, write explicitly $h=P_1^{a_1}\cdots P_r^{a_r}$ for some distinct primes $P_1,\dots,P_r$ and exponents $a_1,\dots,a_r\geq 1$, then

$$H(s,r)=\frac{1}{r!}\sum_{\substack{P_1,\dots,P_r\\ \text{distinct}}}\sum_{\substack{a_1,\dots,a_r\geq 1\\ h=P_1^{a_1}\cdots P_r^{a_r}}}\prod_{i=1}^{r}\left(1+|P_i|^{-1}\right)^{-1}|P_i|^{-2a_i}\sum_{\substack{f_1,\dots,f_s\\ f_1\cdots f_s=h^2}}\frac{\Lambda(f_1)\cdots\Lambda(f_s)}{(\deg f_1)\cdots(\deg f_s)}\,.$$

Since each $f_i$ is a prime power and $f_1\cdots f_s=P_1^{2a_1}\cdots P_r^{2a_r}$, there are finitely many ways to assign prime powers to each $f_i$, according to which we will break $H(s,r)$ into many subsums. With that in mind, for each partition of the set of indexes

$$\{1,2,\dots,s\}=\bigcup_{i=1}^{r}A_i,\quad \#A_i=\lambda_i\geq 1,\forall i,$$

it satisfies the property that

$$\sum_{i=1}^{r}\lambda_i=s\,.$$

We say $(A_1,\dots,A_r)$ is the type of $(f_1,\dots,f_r)$ with $f_1\cdots f_r=h^2$, namely whenever $j\in A_i$, then $f_j$ is a power of $P_i$. Suppose that $f_i=Q_i^{e_i}$ for some prime $Q_i\in\{P_1,\dots,P_r\}$ and exponent $e_i\geq 1$, and the type of $(f_1,\dots,f_r)$ is $(A_1,\dots,A_r)$, since $f_1\cdots f_s=P_1^{2a_1}\cdots P_r^{2a_r}$, comparing the exponents of $P_j$ on both sides we find that

$$\sum_{i\in A_j}e_i=2a_j\ \forall 1\leq j\leq r, \tag{34}$$

and

$$\frac{\Lambda(f_1)\cdots\Lambda(f_s)}{(\deg f_1)\cdots(\deg f_s)}=\frac{1}{e_1\cdots e_s}.$$

Instead of summing over all integers $a_1,\dots,a_r$, we sum over all positive integers $e_1,\dots,e_s$ which satisfy the conditions (34). Noticing that the value only depends

on the vector of integers $(\lambda_1, \dots, \lambda_r)$ such that

$$\sum_{i=1}^{r} \lambda_i = s,$$

hence we can write $H(s,r)$ as

$$H(s,r) = \frac{s!}{r!} \sum_{\substack{\lambda_1+\cdots+\lambda_r=s \\ \lambda_i \geq 1}} \sum_{\substack{P_1,\dots,P_r \\ \text{distinct}}} \prod_{i=1}^{r} \left( \frac{(1+|P_i|^{-1})^{-1}}{\lambda_i!} \sum_{\substack{a_1+\cdots+a_{\lambda_i} \equiv 0 \pmod 2 \\ a_j \geq 1}} \frac{|P_i|^{-a_1-\cdots-a_{\lambda_i}}}{a_1 \cdots a_{\lambda_i}} \right).$$

For each prime $P$ and positive integer $\lambda$, denote

$$\eta(\lambda) = \eta_P(\lambda) := \sum_{\substack{a_1+\cdots+a_\lambda \equiv 0 \pmod 2 \\ a_i \geq 1}} \frac{|P|^{-a_1-\cdots-a_\lambda}}{a_1 \cdots a_\lambda},$$

and

$$\tau(\lambda) = \tau_P(\lambda) := \sum_{\substack{a_1+\cdots+a_\lambda \equiv 1 \pmod 2 \\ a_i \geq 1}} \frac{|P|^{-a_1-\cdots-a_\lambda}}{a_1 \cdots a_\lambda}.$$

Since

$$-\log(1-x) = \sum_{n \geq 1} \frac{x^n}{n}, \quad |x| < 1,$$

we find

$$\eta(1) = -\frac{1}{2} \log\left(1 - |P|^{-2}\right), \tag{35}$$

and

$$\eta(\lambda) + \tau(\lambda) = \sum_{a_1,\cdots a_\lambda \geq 1} \frac{|P|^{-a_1-\cdots-a_\lambda}}{a_1 \cdots a_\lambda} = (-1)^\lambda \log^\lambda\left(1 - |P|^{-1}\right). \tag{36}$$

Combining (35) and (36) we have

$$\tau(1) = -\log\left(1 - |P|^{-1}\right) + \frac{1}{2} \log\left(1 - |P|^{-2}\right).$$

For $\lambda \geq 2$, we can write

$$\eta(\lambda) = \sum_{\substack{a_2+\cdots+a_\lambda \equiv 0 \pmod 2 \\ a_i \geq 1}} \left( \prod_{i=1}^{\lambda} \frac{|P|^{-a_i}}{a_i} \right) \eta(1) + \sum_{\substack{a_2+\cdots+a_\lambda \equiv 1 \pmod 2 \\ a_i \geq 1}} \left( \prod_{i=1}^{\lambda} \frac{|P|^{-a_i}}{a_i} \right) \tau(1).$$

This shows that

$$\eta(\lambda) = \eta(1)\eta(\lambda-1) + \tau(1)\tau(\lambda-1). \tag{37}$$

Similarly for $\lambda \geq 2$,

$$\tau(\lambda) = \eta(1)\tau(\lambda-1) + \tau(1)\eta(\lambda-1). \tag{38}$$

We can assign the initial values

$$\eta(0) = 1, \quad \tau(0) = 0,$$

so that the recursive relations (37) and (38) hold for any $\lambda \geq 1$. Subtracting these two recursive relations we obtain

$$\eta(\lambda) - \tau(\lambda) = (\eta(1) - \tau(1)) (\eta(\lambda-1) - \tau(\lambda-1)).$$

Applying this relation recursively and using (36) we conclude that

$$\eta(\lambda) = \frac{1}{2} \left( u_P^\lambda + (-1)^\lambda v_P^\lambda \right),$$

where

$$u_P = -\log\left(1 - |P|^{-1}\right), \quad v_P = \log\left(1 + |P|^{-1}\right).$$

Therefore $H(s,r)$ can be written as

$$H(s,r) = \frac{s!}{2^r r!} \sum_{\substack{\lambda_1+\cdots+\lambda_r = s \\ \lambda_i \geq 1}} \sum_{\substack{P_1,\ldots,P_r \\ \text{distinct}}} \prod_{i=1}^{r} \frac{u_{P_i}^{\lambda_i} + (-1)^{\lambda_i} v_{P_i}^{\lambda_i}}{\lambda_i! \left(1 + |P_i|^{-1}\right)}.$$

Returning to (33) completes the proof of Proposition 1. □

6.2. **Proposition 2.** We will prove the following.

**Proposition 2.** *For any positive integer $s \geq 4$ we have*

$$H(s) \leq C \left( \frac{4s \log\log s}{\sqrt{q} \log s} \right)^s ,$$

*where $C > 0$ is an absolute constant.*

**Proof.** Denote for each positive integer $\lambda$

$$h(\lambda) = \sum_P \left( u_P^\lambda + (-1)^\lambda v_P^\lambda \right),$$

where the summation is over all monic irreducible polynomials $P \in \mathbb{F}_q[X]$. An upper bound of $H(s,r)$ is given by

$$G(s,r) = \frac{s!}{2^r r!} \sum_{\substack{\lambda_1 + \cdots + \lambda_r = s \\ \lambda_i \geq 1}} \prod_{i=1}^r \frac{h(\lambda_i)}{\lambda_i!} . \tag{39}$$

**Lemma 3.** *For each positive integer $\lambda \geq 2$, we have*

$$h(2+\lambda) < h(2)h(\lambda) .$$

**Proof.** We have

$$h(2)h(\lambda) = \sum_{P,Q} \left( u_P^2 + v_P^2 \right) \left( u_Q^\lambda + (-1)^\lambda v_Q^\lambda \right),$$

hence

$$h(2)h(\lambda) > \sum_{P=Q} \left( u_P^2 + v_P^2 \right) \left( u_P^\lambda + (-1)^\lambda v_P^\lambda \right).$$

Since $u_P > v_P > 0$ for any $P$, we have

$$\left( u_P^2 + v_P^2 \right) \left( u_P^\lambda + (-1)^\lambda v_P^\lambda \right) - \left( u_P^{2+\lambda} + (-1)^\lambda v_P^{2+\lambda} \right) = u_P^2 v_P^2 \left( u_P^{\lambda-2} + (-1)^\lambda v_P^{\lambda-2} \right) \geq 0,$$

hence

$$h(2)h(\lambda) > \sum_P \left(u_P^{2+\lambda} + (-1)^\lambda v_P^{2+\lambda}\right) = h(2+\lambda).$$

This completes the proof of Lemma 3. □

**Lemma 4.**

$$h(3) < h(2)^{3/2}.$$

**Proof.** Since

$$h(2)^3 = \sum_{P,Q,R} \left(u_P^2 + v_P^2\right)\left(u_Q^2 + v_Q^2\right)\left(u_R^2 + v_R^2\right),$$

we have

$$h(2)^3 > \sum_{P,Q=R} \left(u_P^2 + v_P^2\right)\left(u_Q^2 + v_Q^2\right)^2.$$

Similarly,

$$h(2)^3 > \sum_{P=R,Q} \left(u_P^2 + v_P^2\right)^2\left(u_Q^2 + v_Q^2\right).$$

Noting that

$$h(3)^2 = \sum_{P,Q} \left(u_P^3 - v_P^3\right)\left(u_Q^3 - v_Q^3\right) < \sum_{P,Q} u_P^3 u_Q^3,$$

and

$$u_P^3 u_Q^3 \le \frac{1}{2}\left(u_P^2 u_Q^4 + u_P^4 u_Q^2\right) < \frac{1}{2}\left(\left(u_P^2 + v_P^2\right)\left(u_Q^2 + v_Q^2\right)^2 + \left(u_P^2 + v_P^2\right)^2\left(u_Q^2 + v_Q^2\right)\right),$$

summing over all $P$ and $Q$ we find that

$$h(3)^2 < h(2)^3.$$

This completes the proof of Lemma 4. □

**Lemma 5.**

$$h(1) < h(2)^{1/2}.$$

**Proof.** This can be checked explicitly. First

$$h(1) = \sum_P \log \frac{1}{1-|P|^{-2}} = \log \prod_P \left(1-|P|^{-2}\right)^{-1} .$$

From the zeta function of the rational function field $K = \mathbb{F}_q(X)$ we know that

$$\prod_P \left(1-|P|^{-2}\right)^{-1} = \left(1-q^{-1}\right)^{-1},$$

hence

$$h(1) = -\log\left(1-q^{-1}\right) .$$

On the other hand,

$$h(2) = \sum_P \log^2\left(\frac{1}{1-|P|^{-1}}\right) + \log^2\left(1+|P|^{-1}\right). \tag{40}$$

The terms with $\deg P = 1$ (there are $q$ of them) already contribute

$$q\left(\log^2\left(\frac{1}{1-q^{-1}}\right) + \log^2\left(1+q^{-1}\right)\right) > q\log^2\left(\frac{1}{1-q^{-1}}\right)$$

to $h(2)$. This completes the proof of Lemma 5. □

From Lemma 4 and Lemma 5 we know that

$$h(1)^2 h(3)^2 < h(2)h(2)^3 = h(2)^4,$$

hence

$$h(1)h(3) < h(2)^2. \tag{41}$$

Suppose that $s$ is a positive integer. For any positive integers $\lambda_1, \ldots, \lambda_r$ such that

$$\sum_{i=1}^{r} \lambda_i = s,$$

from Lemma 3–5 and using (41), we find that

$$\prod_{i=1}^{r} h(\lambda_i) \leq h(2)^{s/2}\,.$$

Using this in (39) to get an upper bound for $H(r,s)$ and then returning to $H(s)$ in (33), we obtain that for any positive integer $s$,

$$H(s) \leq \sum_{r=1}^{s} \frac{s!h(2)^{s/2}}{2^r r!} \sum_{\substack{\lambda_1+\cdots+\lambda_r=s \\ \lambda_i\geq 1}} \frac{1}{\lambda_1!\cdots\lambda_r!}\,.$$

From definition of $h(2)$ in (40) and using

$$\log(1+x) \leq x, \quad 0<x<1,$$

we find

$$h(2) \leq \sum_{P} \frac{1}{(|P|-1)^2} + \frac{1}{|P|^2}\,.$$

Summing over all monic polynomials $h \in \mathbb{F}_q[X]$ instead of monic irreducible polynomials $P \in \mathbb{F}_q[X]$, we obtain

$$h(2) < \sum_{n=1} q^n \left\{ \frac{1}{(q^n-1)^2} + \frac{1}{q^{2n}} \right\},$$

hence

$$h(2) < \left( \left(1-q^{-1}\right)^{-2} + 1 \right) \sum_{n\geq 1} q^{-n} \leq 10q^{-1}\,.$$

Also from the identity

$$(x_1+\cdots+x_r)^s = \sum_{\substack{\lambda_1+\cdots+\lambda_r=s \\ \lambda_i\geq 0}} \frac{s!}{\lambda_1!\cdots\lambda_r!}\; x_1^{\lambda_1}\cdots x_r^{\lambda_r},$$

we find that

$$\sum_{\substack{\lambda_1+\cdots+\lambda_r=s \\ \lambda_i\geq 1}} \frac{s!}{\lambda_1!\cdots\lambda_r!} < r^s.$$

Therefore

$$H(s) < \sum_{r=1}^{s} \frac{1}{2^r r!} \left( \frac{\sqrt{10}\, r}{\sqrt{q}} \right)^s .$$

To find an upper bound, denote

$$a_r = \frac{r^s}{2^r r!}.$$

Then

$$\frac{a_{r+1}}{a_r} = \frac{1}{2r} \left( 1 + \frac{1}{r} \right)^{s-1} .$$

If $s \geq 100$, we choose

$$l_0 = \left[ \frac{s \log\log s}{\log s} \right].$$

We find that

$$\sum_{r=1}^{l_0} \frac{1}{2^r r!} \left( \frac{\sqrt{10}\, r}{\sqrt{q}} \right)^s \leq \left( \frac{\sqrt{10}\, s \log\log s}{\sqrt{q} \log s} \right)^s \sum_{r=1}^{\infty} \frac{1}{2^r r!} = e^{1/2} \left( \frac{4s \log\log s}{\sqrt{q} \log s} \right)^s .$$

For the choice of $l_0$ we have

$$l_0 \log l_0 = s \log\log s \, (1 + o_s(1)) \geq s,$$

and from it we derive

$$\frac{a_{r+1}}{a_r} \leq \frac{1}{2}, \quad \forall r \geq l_0.$$

Hence

$$\sum_{r=l_0}^{s} \frac{1}{2^r r!} \left( \frac{\sqrt{10}\, r}{\sqrt{q}} \right)^s \leq \frac{1}{2^{l_0} l_0!} \left( \frac{\sqrt{10}\, l_0}{\sqrt{q}} \right)^s \left( 1 + 2^{-1} + 2^{-2} + \cdots \right) \leq \left( \frac{\sqrt{10}\, s \log\log s}{\sqrt{q} \log s} \right)^s .$$

Therefore

$$H(s) \leq 3 \left( \frac{\sqrt{10}\, s \log\log s}{\sqrt{q} \log s} \right)^s$$

for any positive integer $s \geq 100$. On the other hand, if $4 \leq s < 100$, we use the trivial estimate

$$H(s) < \left(\frac{\sqrt{10}\, s}{\sqrt{q}}\right)^s \sum_{r=0}^{\infty} \frac{1}{2^r r!} = e^{1/2} \left(\frac{\sqrt{10}\, s}{\sqrt{q}}\right)^s,$$

this again is bounded by $C\left(\frac{\sqrt{10}\, s \log\log s}{\sqrt{q}\log s}\right)^s$ for some absolute constant $C > 0$ for $4 \leq s < 100$. This completes the proof of Proposition 2. $\square$

6.3. **Proposition 3.** Finally, we prove the following.

**Proposition 3.** *If $s$ is a fixed positive integer, then*

$$H(s) = \frac{\delta_{s/2}\, s!}{2^{r/2}(s/2)!}\, q^{-s/2} + O_s\left(q^{-(s+1)/2}\right),$$

*as $q \to \infty$, where for any $\gamma \in \mathbb{R}$,*

$$\delta_\gamma = \begin{cases} 1 & \gamma \in \mathbb{Z}, \\ 0 & \gamma \notin \mathbb{Z}. \end{cases}$$

**Proof.** For any $\lambda \in \mathbb{N}$ and $P \in \mathbb{F}_q[X]$, denote

$$g(\lambda, |P|) = \frac{u_P^\lambda + (-1)^\lambda v_P^\lambda}{1 + |P|^{-1}},$$

where $u_P$ and $v_P$ are given in (32). We use Taylor series expansions of $-\log(1-x)$ and $\log(1+x)$ ($|x| \leq 1/2$) given by

$$-\log(1-x) = x + \frac{x^2}{x} + \frac{x^3}{3} + \cdots = x\left(1 + \frac{x}{2} + O(x^2)\right),$$

and

$$\log(1+x) = x - \frac{x^2}{x} + \frac{x^3}{3} + \cdots = x\left(1 - \frac{x}{2} + O(x^2)\right)$$

to deduce

$$g(\lambda,|P|)=\begin{cases} 2|P|^{-\lambda}\left(1+O\left(|P|^{-1}\right)\right) & : \ \lambda\equiv 0 \pmod 2,\\ \lambda|P|^{-\lambda-1}\left(1+O\left(|P|^{-1}\right)\right) & : \ \lambda\equiv 1 \pmod 2.\end{cases} \tag{42}$$

For any $n\in\mathbb{N}$, denote

$$\pi_q(n)=\#\{P\in\mathbb{F}_q[X]: P \text{ is monic, irreducible and } \deg P=n\}.$$

It is known ([17]) that

$$\pi_q(n)=\frac{q^n}{n}\left(1+O(q^{-n/2})\right). \tag{43}$$

Fix a positive integer $s$. For any positive integer $\lambda\le s$, denote

$$z(\lambda)=\sum_P g(\lambda,|P|)=\sum_{n\ge 1} g(\lambda,q^n)\pi_q(n).$$

If $\lambda$ is even, from (42)

$$z(\lambda)=\sum_{n\ge 1}\frac{2q^{-n\lambda}\left(1+O(q^{-n})\right)}{1+q^{-n}}\pi_q(n).$$

For $n=1$, since $\pi_q(1)=q$, this gives us the value $2q^{-\lambda+1}\left(1+O(q^{-1})\right)$. For $n\ge 2$, using (43) and noting that $\lambda\ge 2$, we find that all such terms added together contribute to a value bounded by $O(q^{-\lambda})$. Hence

$$z(\lambda)=2q^{-\lambda+1}\left(1+O_s(q^{-1})\right), \quad \text{if } \lambda\equiv 0 \pmod 2. \tag{44}$$

The notation "$O_s$" in the above formula is to stress that the implied constant may depend on the value $s$ since $1\le\lambda\le s$. Similarly if $\lambda$ is odd, we obtain that

$$z(\lambda)=\lambda q^{-\lambda}\left(1+O_s(q^{-1})\right), \quad \text{if } \lambda\equiv 1 \pmod 2. \tag{45}$$

We write

$$H(s) = \sum_{r=1}^{s} \frac{s!}{2^r r!} \sum_{\substack{\lambda_1+\cdots+\lambda_r=s \\ \lambda_i \geq 1}} f(\lambda_1, \ldots, \lambda_r)\,, \tag{46}$$

where

$$f(\lambda_1, \ldots, \lambda_r) = \sum_{\substack{P_1,\ldots,P_r \\ \text{distinct}}} \prod_{i=1}^{r} \frac{g(\lambda_i, |P_i|)}{\lambda_i!}\,.$$

For any positive integers $\lambda_1, \ldots, \lambda_r$ with

$$\sum_{i=1}^{r} \lambda_i = s,$$

denote

$$\{1, 2, \ldots, r\} = A \bigcup B,$$

where

$$A = \{1 \leq i \leq r : \lambda_i \text{ is even}\}, \quad B = \{1 \leq i \leq r : \lambda_i \text{ is odd}\}.$$

Since for any $i \in A$, $\lambda_i \geq 2$, and

$$s = \sum_{i \in A} \lambda_i + \sum_{i \in B} \lambda_i,$$

we check that if $\#B \geq 1$ then $\#A \leq (s-1)/2$, or if there is an $i \in A$ with $\lambda_i \geq 4$, then $\#A \leq (s-2)/2$. In either of these cases, since

$$f(\lambda_1, \ldots, \lambda_r) \leq \left(\prod_{i \in A} z(\lambda_i)\right)\left(\prod_{i \in B} z(\lambda_i)\right),$$

using (44) and (45) we obtain

$$f(\lambda_1, \ldots, \lambda_r) \ll_s \left(\prod_{i \in A} q^{-\lambda_i+1}\right)\left(\prod_{i \in B} q^{-\lambda_i}\right) = q^{-s+\#A} \leq q^{-(s+1)/2}\,.$$

The case that is not covered by the above consideration is that $\#B = 0$ and there is no $i \in A$ with $\lambda_i \geq 4$, that is, $\lambda_i = 2$ for any $1 \leq i \leq r$. That means that $s = 2r$ is even. The only term left is

$$f(2,\dots,2) = \frac{1}{2^r} \sum_{\substack{P_1,\dots,P_r \\ \text{distinct}}} \prod_{i=1}^{r} g\left(2,|P_i|\right) . \tag{47}$$

Since

$$\sum_{\substack{P_1,\dots,P_r \\ \text{not distinct}}} \prod_{i=1}^{r} g\left(2,|P_i|\right) \ll_s \sum_{\substack{P_1,\dots,P_r \\ P_1=P_2}} \prod_{i=1}^{r} g\left(2,|P_i|\right) = \left(\sum_P g\left(2,|P|\right)^2\right)\left(\sum_P g\left(2,|P|\right)\right)^{r-2},$$

and we can check easily that

$$\sum_P g\left(2,P\right)^2 \ll q^{-3}.$$

Using the above and (44) we find that removing the restrictions that $P_1,\dots,P_r$ are distinct in (47) would result in an error bounded by $O_s\left(q^{-r-1}\right) = O_s\left(q^{-(s+1)/2}\right)$. The main term in (47) is given by

$$\frac{1}{2^r}\left(\sum_P g\left(2,|P|\right)\right)^r = q^{-r}\left(1+O_s(q^{-1})\right) = q^{-s/2}\left(1+O_s(q^{-1})\right) .$$

Combining all the above computation together and returning to (46), we conclude that

$$H(s) = \frac{\delta_{s/2}\, s!}{2^{r/2}(s/2)!}\, q^{-s/2} + O_s\left(q^{-(s+1)/2}\right) ,$$

as $q \to \infty$. This completes the proof of Proposition 3. $\square$

## References

[1] J.D. Achter, *The distribution of class groups of function fields*, J. Pure Appl. Algebra **204** (2006), no. 2, 316–333.

[2] J.D. Achter, *Results of Cohen-Lenstra type for quadratic function fields*, Computational arithmetic geometry, 1–7, Contemp. Math., **463**, Amer. Math. Soc., Providence, RI, 2008.

[3] L.M. Adleman, M.A. Huang, "Primality testing and abelian varieties over finite fields", Lecture Notes in Mathematics, 1512.

[4] A. Bucur, C. David, B. Feigon, M. Lalín, *Statistics for traces of cyclic trigonal curves over finite fields*, International Mathematics Research Notices (2010), 932–967.

[5] A. Bucur, C. David, B. Feigon, M. Lalín, *Biased statistics for traces of cyclic p-fold covers over finite fields*, to appear in Proceedings of Women in Numbers, Fields Institute Communications.

[6] M. Deuring. *Die Typen der Multiplikatorenringe elliptischer Funktionenkö per*, Abh. Math. Sem. Hansischen Univ., **14** (1941), 197–272.

[7] P. Diaconis, S. Evans, *Linear functionals of eigenvalues of random matrices*, Trans. Amer. Math. Soc. **353** (2001), no. 7, 2615–2633.

[8] D. Faifman, Z. Rudnick, *Statistics of the zeros of zeta functions in families of hyperelliptic curves over a finite field*, arXiv:0803.3534. To appear in Compositio Math.

[9] N. M. Katz, P. Sarnak, "Random Matrices, Frobenius Eigenvalues, and Monodromy", Amer. Math. Soc. Colloq. Publ., vol. 45, American Mathematical Socitey, Providence, RI, 1999.

[10] P. Kurlberg, Z. Rudnick, *The fluctuations in the number of points on a hyperelliptic curve over a finite field*, J. Number Theory Vol. 129 **3** (2009), 580-587.

[11] H. W. Lenstra, Jr., J. Pila, C. Pomerance, *A hyperelliptic smoothness test. I*, Philos. Trans. Roy. Soc. London Ser. A **345** (1993), no. 1676, 397–408.

[12] H. W. Lenstra, Jr., *Factoring integers with elliptic curves*, Ann. of Math. (2) **126** (1987), no. 3, 649–673.

[13] D. Lorenzini, "An invitation to arithmetic geometry", Graduate Studies in Mathematics, 9. American Mathematical Society, Providence, RI, 1996.

[14] C. Moreno, "Algebraic curves over finite fields", Cambridge Tracts in Mathematics **97**, Cambridge University Press, 1991.

[15] H.G. Quebbemann. *Estimates of regulators and class numbers in function fields*, J. Reine Angew. Math., **419** (1991), 79–87.

[16] M.Y. Rosenbloom, M.A. Tsfasman, *Multiplicative lattices in global fields*, Invent. Math., **101** (1990), 687–696.

[17] M. Rosen, "Number theory in function fields". Graduate Texts in Mathematics, **210**. Springer-Verlag, New York, 2002.

[18] Z. Rudnick, *Traces of high powers of the Frobenius class in the hyperelliptic ensemble*, Acta Arith. **143** (2010), 81-99.

[19] I. Shparlinski, *On the size of the Jacobians of curves over finite fields*, Bull. Braz. Math. Soc. (N.S.) **39** (2008), no. 4, 587–595.

[20] A. Stein, E. Teske. *Explicit bounds and heuristics on class numbers in hyperelliptic function fields*, Math. Comp., **71** (2002), 837–861.

[21] M. Tsfasman, *Some remarks on the asymptotic number of points*, Coding theory and algebraic geometry (Luminy, 1991). Lect. Notes in Math., vol. 1518, Springer, (1992), 178–192.

[22] A. Venkatesh, S. Ellenberg, *Statistics of number fields and function fields*, Proceedings of the International Congress of Mathematicians Hyderabad, India, 2010.

[23] A. Weil, *Sur les Courbes Algébriques et les Variétés qui s'en Déduisent*, Publ. Inst. Math. Univ. Strasbourg **7** (1945), Hermann et Cie., Paris, 1948.

Maosheng Xiong: Department of Mathematics, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, P. R. China

*E-mail address*: mamsxiong@ust.hk

Alexandru Zaharescu: Institute of Mathematics of the Romanian Academy, P.O. Box 1–764, 70700 Bucharest, Romania, and Department of Mathematics, University of Illinois at Urbana-Champaign, 273 Altgeld Hall, MC-382, 1409 W. Green Street, Urbana, IL 61801 USA

*E-mail address*: zaharesc@math.uiuc.edu